

WHAT IS CLAIMED IS:

1. A method of controlling distribution of a segment of encrypted electronic information, comprising:

- 5 receiving, from a key server, a protected decryption key associated with the segment;  
retrieving, at a user location, the segment;  
obtaining an unprotected copy of the decryption key from the protected decryption key;  
10 decrypting, in response to said obtaining, the segment using the unprotected copy of the decryption key;  
destroying the unprotected copy of the decryption key at the user location in response to said decrypting;  
displaying the decrypted segment in response to said decrypting; and  
15 destroying the decrypted segment in response to said displaying.

2. The method of claim 1, further comprising:

- saving, in response to said receiving, the protected decryption key;  
wherein said destroying the unprotected copy of the decryption key does not  
20 effect the unprotected copy of the decryption key.

3. The method of claim 1, further comprising:

- said receiving further comprising receiving at least one access policy associated with at least one of the key server, the user location, the segment, the  
25 decryption key, and a user, the at least one access policy including at least one fixed time limitation;  
said determining comprising determining whether current operating conditions, including the current time, satisfy the at least one access policy.

30

4. The method of claim 1, further comprising:  
 saving, in response to said receiving, the protected decryption key in memory;  
 and  
 rendering the protected copy of the decryption key inaccessible after an  
 expiration time in the at least one access policy.

5. A method for issuing a key lease, comprising:  
 receiving, at a remote server, a request to lease a decryption key for an encrypted  
 electronic segment;  
 determining whether a key lease can be issued for the encrypted electronic  
 information based on at least one of a remote server restriction, an  
 information restriction, and a user restriction;  
 creating a voucher in response to a determination that the key lease can be issued,  
 said voucher including at least the decryption key, and at least one time  
 limitation associated with the decryption key;  
 encrypting at least the decryption key of the voucher; and  
 sending the voucher to the user location.

6. The method of claim 5, wherein said creating further comprises adding access  
 policies associated with the information to the voucher.

7. The method of claim 5, wherein said receiving further comprises receiving a  
 requested time frame of use of the key lease, and wherein the at least one  
 time limitation includes an expiration time based on at least one of a  
 maximum allowed by the remote server, a maximum allowed by the  
 information, a maximum allowed by user limitations, and the requested  
 time frame.



destroying, in response to said accessing, the decrypted copy of the decryption key.

13. The method of claim 12, further comprising:

5 displaying the accessed segment in response to said accessing; and  
destroying the accessed segment in response to said displaying.

14. The method of claim 12, wherein the voucher includes access policies, the method further comprises:

10 determining, in response to said decrypting, whether operating parameters satisfy the access policies; and  
said accessing being responsive to said operating parameters being determined to satisfy the access policies;  
wherein said accessing is responsive to said decrypting through said determining.

15 15. A method for controlling distribution of electronic information, comprising:  
retrieving, at a user location, a segment of encrypted electronic information;  
receiving, from a key server, an encrypted decryption key for the segment;  
saving said encrypted decryption key in a memory;  
20 obtaining a decrypted copy of the decryption key in response to an authorized user request to access the segment;  
accessing the segment using the decrypted copy of the decryption key at the user location for the segment; and  
destroying the decrypted copy of the decryption key at the user location in  
25 response to said accessing without destroying the encrypted decryption key in memory.

16. The method of claim 15, further comprising:

30 displaying the decrypted segment in response to said accessing; and  
destroying the decrypted segment in response to one of said displaying.

009427 " 62333.260

17. A method of accessing a protected segment of electronic information, the  
segment having an associated key, comprising:  
retrieving, at the user location, the segment;  
5 receiving, at the user location from the remote server, the key;  
accessing the segment, in response to said receiving, using the key;  
displaying the segment as accessed;  
destroying the key in response to one of said displaying and said accessing,  
wherein the key is never stored in memory at a user location between said  
10 receiving and said destroying;  
receiving, at the user location from the remote server, an encrypted key lease  
including the key;  
saving the encrypted key lease in a memory;  
breaking a connection between the user location and the remote server; and  
15 during a period of the broken connection:  
retrieving, at the user location, the segment;  
obtaining a decrypted copy of the key from the key lease;  
accessing the segment in response to said obtaining;  
displaying the segment as accessed; and  
20 destroying the decrypted copy of the key in response to one of said  
displaying and said accessing.

18. The method of claim 17, further comprising restoring a connection between  
the user location and the remote server.

19. The method of claim 18, further comprising revoking the key lease after said  
restoring.

20. The method of claim 18, further comprising:  
logging said obtaining in a log; and  
sending, after said restoring, the log from the user location to the remote server.

5 21. The method of claim 20, further comprising detecting, at one of the user  
location and the remote server, from the contents of the log, any  
tampering at the user location relating to at least one of the key lease, the  
segment, and operating conditions at the user location.

10 22. A method of viewing a segment of encrypted electronic information on a  
display, comprising:

receiving, from a remote server, an encrypted decryption key for the segment;  
retrieving, at a user location, a segment of encrypted electronic information;  
first decrypting the encrypted decryption key in response to the presence of  
15 authorized conditions;

second decrypting the segment using the decrypted decryption key;  
destroying, at the user location, all copies of the decrypted decryption key in  
response to said second decrypting, without destroying the encrypted  
decryption key;

20 displaying the segment as decrypted on the display; and  
destroying, at the user location, the segment as decrypted in response to said  
displaying.

23. A method of controlling distribution of a segment of encrypted electronic  
25 information, the segment having a first and second portion, the method  
comprising:

receiving, from a key server, an encrypted voucher, the voucher including first  
and second decryption keys associated with the first and second portions,  
respectively,

30 retrieving, at a user location, the segment;

accessing the protected copy of the first decryption key;  
 decrypting, in response to said accessing, the first portion of the segment using  
 the accessed copy of the first decryption key;  
 destroying the accessed copy of the first decryption key at the user location in  
 5 response to said decrypting;  
 displaying the decrypted segment in response to one of said decrypting and said  
 destroying;  
 destroying the decrypted first portion in response to said displaying;  
 accessing the protected copy of the second decryption key after said destroying  
 10 the first decrypted segment; and  
 decrypting, in response to said accessing the protected copy of the second  
 decryption key, the second portion of the segment using the accessed copy  
 of the second decryption key.

15 24. A method of limiting access to a segment of encrypted information,  
 comprising:  
 saving, at a remote server, a decryption key for the segment, the segment being at  
 a location other than the remote server;  
 receiving a request from an authorized user for the decryption key;  
 20 sending a copy of the decryption key from the remote server to a source of the  
 request;  
 destroying the decryption key at the remote server in response to the elapse of a  
 predetermined period of time.

25 25. The method of claim 24, further comprising preventing the source from  
 storing the copy of the decryption key, wherein said destroying leaves  
 said segment permanently inaccessible absent breaking of the encryption  
 protecting of the segment.

